THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NS/EP IMPLICATIONS OF ELECTRONIC COMMERCE

JUNE 1999

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 01061999	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle NS/EP Implications of Electronic Commerce Procedures	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es) Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 42	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	6/1/99	Report

4. TITLE AND SUBTITLE
NS/EP Implications of Electronic Commerce

5. FUNDING NUMBERS

6. AUTHOR(S)
President's National Security Telecommunications Advisory Committee

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This analysis focuses primarily on NS/EP issues related to recent activities within the Federal Government to incorporate EC into business operations. In particular, the NSTAC focused on how the transition to EC could affect the departments and agencies that conduct NS/EP functions.

14. SUBJECT TERMS
Electronic Warfare

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

NS/EP IMPLICATIONS OF ELECTRONIC COMMERCE
TABLE OF CONTENTS

EXECUTIVE SUMMARY ES-1

1.0 INTRODUCTION 1

1.1 Background 1
1.2 Purpose and Scope 1
1.3 Definitions 2
1.4 Approach 3

2.0 THE ELECTRONIC COMMERCE ENVIRONMENT 4

2.1 Commercial Use of Electronic Commerce 4
2.2 Electronic Commerce in the Federal Government 6
2.2.1 Framework for Global Electronic Commerce 6
2.2.2 Initiatives to Incorporate EC Within the Federal Government 6

3.0 ELECTRONIC COMMERCE SECURITY 11

3.1 Security Objectives 11
3.2 The EC Architecture 12
3.3 Threats to the EC Architecture 15

4.0 FACTORS AFFECTING ELECTRONIC COMMERCE RISK 18

4.1 Speed of Business 18
4.2 Rate of Technology Change 18
4.3 Commercial-Off-the-Shelf Products 19
4.4 Federal Government Information Security 20
4.5 Coordination of EC Initiatives 21
4.6 Risk Approaches 21

5.0 CONCLUSIONS 23

5.1 Anticipated Growth of NS/EP Dependence on EC 23
5.2 Exposure to EC Risks and Vulnerabilities 24
5.3 Understanding NS/EP Dependence on EC 24
5.4 Shared Risk 25
5.5 Lack of Unified Focus on NS/EP-Specific Needs 25

6.0 RECOMMENDATIONS 27

6.1 NSTAC Recommendations to the President 27
6.2 NSTAC Direction to the IES 28

CONTINUED

APPENDIX A: REPORT CONTRIBUTORS A-1

APPENDIX B: REFERENCES B-1

EXECUTIVE SUMMARY

Background

The public sector is in the midst of adopting system-wide changes that will incorporate electronic commerce (EC) into Government operations. A number of Federal Government agencies are currently investigating how EC technologies can be used to streamline their business operations. For example, at the President's National Security Telecommunications Advisory Committee's (NSTAC) 20th meeting, the Honorable John Hamre, Deputy Secretary of Defense, expressed the intent of the Department of Defense (DOD) to move toward a paperless operation, using EC technologies and state-of-the-art security tools and strategies. Dr. Hamre noted that moving DOD to a paperless environment is one of his top priorities. The DOD initiative to incorporate EC into business operations represents the first large-scale effort toward EC by a member of the national security and emergency preparedness (NS/EP) community.

The Information Infrastructure Group (IIG) formed the EC Subgroup to investigate the implications of incorporating EC into business operations within the NS/EP community. The EC Subgroup focused its efforts on the changing business and security processes and policies necessary to adopt EC and the potential implications those changes might have for NS/EP operations. Toward that end, the IIG surveyed diverse EC literature from Government, industry, and academic sources. In addition, the IIG received a variety of briefings from Government, industry, and academia related to the EC environment, how EC is being incorporated by the public and private sectors, and EC security concerns. Finally, to gain greater insight into potential NS/EP implications of incorporating EC into business operations, the IIG interviewed public and private sector officials responsible for implementing EC policies and procedures.

Various departments and agencies within the Federal Government have used different forms of EC and Electronic Data Interchange (EDI) for a number of years. However, recent Federal EC initiatives mark a change from previous efforts in terms of scale and technologies used. These efforts mark one of the first steps toward incorporating EC Government-wide. Additionally, the initiatives move away from using Government-developed technologies and standards toward using commercial products and standards, where the Government has little, if any, control over their development. As dependence on the Internet and data networks increases, and as EC applications become more pervasive throughout Government and industry, EC could become a critical element in supporting the NS/EP posture of the Nation.

Conclusions

This analysis focuses primarily on NS/EP issues related to recent activities within the Federal Government to incorporate EC into business operations. In particular, the NSTAC focused on how the transition to EC could affect the departments and agencies that conduct NS/EP

functions. Currently, EC use among such organizations has been limited to the support of non-mission critical activities. However, as NS/EP organizations increase their reliance on EC for contracting, ordering and distributing essential supplies in support of the public welfare, national security posture, or any other NS/EP function, the security of these transactions will become more critical to NS/EP operations. As the NS/EP community transitions to EC for business operations, the departments and agencies should be alert to a number of issues that could affect how EC is implemented.

- Initial analysis shows that the NS/EP community's current use of, and dependence on, EC is modest at best. However, a number of factors will drive the NS/EP community to use EC to support its mission. Consequently, NS/EP dependence on EC, although modest at present, is likely to grow steadily over the next decade.

- EC exposes what were once closed and paper-based business processes to the vulnerabilities of EC hardware and software and supporting information technologies. It is important for the NS/EP community to be aware of these vulnerabilities and make informed decisions regarding how EC technologies should be implemented to achieve an acceptable level of risk.

- The NS/EP community may not fully understand its current or future EC dependencies. It is important that NS/EP departments and agencies thoroughly assess current and future dependence on EC applications and architectures, the associated security implications, and the effect EC will have on overall business operations.

- It is critical to note that in the new electronic environment created by EC, the NS/EP community will depend on commercial products and an information infrastructure that it neither owns nor operates. Therefore, the Federal Government and its partners in the private sector will share the NS/EP risks involved with EC.

- There is a lack of a unified and specific focus on NS/EP needs among organizations responsible for managing and administering oversight for EC within the Federal Government such as the Federal Electronic Commerce Program Office (FECPO), The Joint Electronic Commerce Program Office (JECPO), President's Management Council (PMC), Office of Federal Procurement Policy (OFPP), and Federal Electronic Commerce Acquisition Team (ECAT). This lack of focus could lead to a lack of formal guidance, policy, procedures, and accountability addressing NS/EP issues related to the adoption of EC.

Recommendations

This analysis reflects the importance of encouraging a broader awareness of NS/EP issues related to the introduction of EC. The NSTAC has found a lack of focus on NS/EP needs within these various entities. Therefore, there is a need to establish a focal point within the Federal Government to work with these various public and private organizations to increase their awareness of NS/EP issues related to EC.

Our analysis has also found a need to increase the NS/EP community's awareness of the potential vulnerabilities related to EC. Federal departments and agencies should work with a focal point within the Federal Government to evaluate their current and future dependence on EC for NS/EP mission-critical operations and develop plans and programs to address the vulnerabilities related to incorporating EC into business operations. Departments and agencies need to develop a thorough understanding of their existing information architectures as well as vulnerabilities caused by the introduction of EC. Once identified, plans and programs can be established to protect their systems.

NSTAC Recommendations to the President

- Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, designate a focal point for examining the NS/EP issues related to widespread adoption of EC within the Government.

The NSTAC's Network Group has developed recommendations proposed to help increase the NS/EP community's awareness and understanding of Internet dependencies, technologies, and vulnerabilities, and to encourage NS/EP awareness among Internet organizations and initiatives. In particular, one recommendation states that, *"Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, direct the establishment of a permanent program to address NS/EP issues related to the Internet."* The IIG endorses the recommendations to establish such a program and believes such a program would satisfy this recommendation.

- Recommend that the President direct that Federal departments and agencies, in cooperation with an established Federal focal point, assess the effect of EC technologies on their NS/EP operations.

NSTAC Direction to the IES

NSTAC directs the Industry Executive Subcommittee (IES) to support the Government's efforts in raising awareness of NS/EP issues related to EC.

1.0 INTRODUCTION

This introduction provides a background on the growth of electronic commerce (EC), outlines the purpose and scope of the issue analysis, presents key definitions used for the analysis, and summarizes the approach taken by the President's National Security Telecommunications Advisory Committee (NSTAC) to determine potential national security and emergency preparedness (NS/EP) implications related to EC.

1.1 Background

Advances in information technology are dramatically altering the way people communicate and conduct business. In the last 5 years in particular, the development of the Global Information Infrastructure (GII), advances in Internet technology, and increased use of the World Wide Web (the Web) have fueled the growth of trade, or EC, over the Internet. EC offers the potential to dramatically increase efficiency and reduce the costs of conducting business. As a result, many public and private organizations have adopted EC applications to increase sales, cut costs, and streamline logistics. However, as EC drives large-scale changes in business practices, organizations are increasingly concerned about the security of EC applications and transactions. New technologies have made critical networks more open and pervasive, introducing a host of vulnerabilities. Before EC can realize its full potential, key partners must have confidence in the confidentiality, integrity, availability, reliability, and authenticity of the transactions conducted using EC applications and networks.

Although the private sector has been the driving force in the growth of EC, the public sector is in the midst of adopting system-wide changes that will incorporate EC into Government operations. A number of Federal Government agencies are investigating how to use EC technologies to streamline their operations. For example, at the NSTAC's 20th meeting, the Honorable John Hamre, Deputy Secretary of Defense, expressed the intent of the Department of Defense (DOD) to move toward a paperless operation, using EC technologies and state-of-the-art security tools and strategies. Dr. Hamre noted that moving DOD to a paperless environment is one of his top goals.

1.2 Purpose and Scope

The DOD initiative to incorporate EC into business operations represents the first large-scale effort toward EC by a member of the NS/EP community. Since 1982, the NSTAC has addressed important issues related to the security of telecommunications and networked technologies and how those issues affect telecommunications services essential to the NS/EP community. NSTAC's Information Infrastructure Group (IIG) formed the EC Subgroup to investigate the implications of incorporating EC into business operations within the NS/EP community. There are a number of issues regarding the overall security of EC and how it relates to the economic security of the Nation. Several other reports have dealt with various EC issues; this

analysis focuses explicitly on how EC will affect NS/EP operations. As dependence on the Internet and data networks increases, and as EC applications become more pervasive throughout Government and industry, EC could become a critical element in supporting the NS/EP posture of the Nation. Currently, EC use among such organizations has been limited to the support of non-mission critical activities. However, as NS/EP organizations increase their reliance on EC for ordering and distributing essential supplies in support of the public welfare, national security posture, or any other NS/EP function, the security of these transactions will become more critical to NS/EP operations.

Since 1990, NSTAC has studied network security issues affecting the foundation of the U.S. telecommunications infrastructure, namely the Public Network (PN).[1] The PN has remained the NSTAC's primary focus of study because of our Nation's increasing reliance on this infrastructure to support NS/EP telecommunications. This increasing reliance on the PN is driven by not only new and improved capabilities and efficiencies offered by these technologies but also the PN's interdependence with other critical infrastructures. Because of these trends in dependencies, the NSTAC has expanded its focus to include key capabilities that rely on the PN. Rather than addressing specific vulnerabilities affecting the PN or Internet as EC enablers, this work focuses on the issues associated with the changing business and security processes and policies necessary to adopt EC.[2]

1.3 Definitions

The NSTAC based its study on two key concepts: "electronic commerce" and "NS/EP telecommunications." The definition of EC varies widely among various EC reports produced by Government, industry, and academia. Because the subgroup was tasked to investigate how EC could affect critical NS/EP operations, the definition used by DOD's Joint Electronic Commerce Program Office (JECPO) was found to be the most applicable. For this analysis, electronic commerce is defined as follows:

> *The paperless exchange of business information using Electronic Data Interchange (EDI), electronic mail (e-mail), computer bulletin boards, FAX, electronic funds transfer (EFT), and other similar technologies.*[3]

In defining NS/EP telecommunications, the subgroup relied upon the National Communications System's (NCS) Telecommunications Service Priority (TSP) Program, which defines NS/EP

[1] The PN includes any switching system or voice, data, or video transmission system used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signaling networks). NSIE, "An Assessment of the Risk to the Security of the Public Networks." Prepared by the U.S. Government and NSTAC Network Security Information Exchanges, December 12, 1995.

[2] The NSTAC is conducting separate studies to address the PN and the Internet. The Government and NSTAC NSIEs are addressing the risk to the PN, and the NSTAC's Network Group is addressing NS/EP dependence on the Internet.

[3] Joint Electronic Commerce Program Office (JECPO), EC/EDI Handbook. http://www.acq.osd.mil/ec/newhandbook/chapter2/chapter2.htm

telecommunications as follows:

> *Services critical to the maintenance of a state of readiness or the response to and management of any event or crisis that causes or could cause harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States.*[4]

1.4 Approach

To complete the task of investigating potential NS/EP implications of EC, the IIG EC Subgroup took the following steps:

- The NSTAC canvassed a broad collection of EC literature produced by Government, industry, and academic sources.

- A variety of officials from Government, industry, and academia briefed the NSTAC on issues related to the EC environment, how EC is being incorporated by the public and private sectors, and concerns regarding EC security.

- To gain greater insight into potential NS/EP implications of incorporating EC into business operations, interviews were conducted with key officials responsible for implementing Federal EC policies and procedures.

[4] National Communications System. Office of Priority Telecommunications (OPT). *Telecommunications Service Priority (TSP) Program Service Manual*. NCSM 3-1-1, March 1998.

2.0 THE ELECTRONIC COMMERCE ENVIRONMENT

Recent advances in information technology have driven what many information technology professionals call a digital revolution, altering how the world communicates and conducts business. In particular, the growth in the use and sophistication of Internet technologies has encouraged a dramatic rise in the use of EC applications for business operations within the private sector and more recently within the public sector.

2.1 Commercial Use of Electronic Commerce

The use of information technology and data networks to facilitate commercial transactions is not a new practice. For nearly 30 years, various public and private sector organizations have used EDI to coordinate purchasing, logistics, sales, and customer service. EDI is the computer-to-computer exchange of business information using private communications networks such as value-added networks (VAN). EDI never met its full potential, however, because the cost of installing, maintaining, and purchasing services on VANs was too high for small to medium-size organizations. Larger organizations that could afford the investment in VANs often found that many of their business partners did not use EDI.

Dramatic advances in information technology (IT) during the last 5 years have expanded the concept of EDI. More recently these advances have enabled the use of EC applications in daily business operations. This change has broadened the definition of EC to include the overall paperless exchange of business information using various electronic methods. The following driving factors have led EC to be used by a much wider audience:

- advances in telecommunications and information technologies,
- increased public accessibility (e.g., the Internet and the Web), and use of personal computers (PC) and software, and
- increasing use of efficiency-driven business practices (e.g., just-in-time inventory).

Increased use of the Internet, in particular, has spurred EC growth. The number of Americans using the Internet has increased from fewer than 5 million in 1993 to nearly 62 million in 1997.[5] UUNET estimates that Internet traffic doubles every 100 days.[6] The number of registered domain names increased from 26,000 in July 1993 to 1.3 million in 1997. In 1995, top-level commercial (.com) domain names accounted for more than 27,000 names, most representing Web sites presenting product or company information. Two years later, the number of

[5] Department of Commerce. *The Emerging Digital Economy*. March 1998, p. 8.
[6] Ibid., p. 8.

commercial domain names increased to 764,000 representing Web sites offering diversified services including business transactions, news and information, and tangible goods.[7]

The types of transactions that can be conducted using EC have grown over the past 3 years. Business transactions conducted using EC can be generally categorized in three areas:

- *Digital delivery of goods and services:* Internet and EC technologies allow for goods and services to be delivered in digital form. These services include providing news and information, downloading software, conducting banking transactions, purchasing airline tickets, and buying insurance. IT industry experts predict that the market for these services will increase significantly in the next few years.[8]

- *Retail sale of tangible goods:* More consumers are using the Web to buy tangible goods. A 1997 CommerceNet/Nielsen study reported that the Internet makes it easier for consumers to research prices and offers a convenient means to buy items. Nearly 10 million users in the United States and Canada have claimed that they purchased an item using the Web.[9]

- *EC among businesses:* Internet commerce among businesses accounts for the largest and fastest growing percentage of EC. Organizations are using EC to coordinate purchasing with suppliers, logistics, sales, and customer service. Business-to-business EC gives companies practical real-time connections with business partners; reduces purchasing costs, cycle times, and marketing costs; reduces inventories; and provides more efficient customer service. It is estimated that by 2002, businesses will trade more than $300 billion in goods and services using EC.[10]

EC offers many potential benefits for organizations interested in increased efficiency and expanded business opportunities. However, concerns regarding Internet security and the lack of consistent business and legal frameworks could inhibit EC's full potential. As a result, organizations using EC applications are working to establish sound legal frameworks and business standards.

[7] Ibid., p. 8.
[8] Ibid., p. 33.
[9] Ibid., p. 35.
[10] Erwin, Blane, et al., *Sizing Intercompany Commerce*, Forrester Research, July 1997.

2.2 Electronic Commerce in the Federal Government

The Federal Government has taken note of commercial trends involved with EC and is determining how it can also exploit the benefits of EC. A number of initiatives show how the Federal Government is planning to incorporate EC into business operations. These initiatives include the U.S. Working Group on Electronic Commerce, the National Performance Review, President's Management Council, DOD, Federal Electronic Commerce Program Office (FECPO), and *Government Paperwork Elimination Act of 1998*.

2.2.1 Framework for Global Electronic Commerce

In December 1995, President Clinton created the U.S. Working Group on Electronic Commerce. This signaled to Government and industry that the Internet and EC would have a strong role in the Administration's policy agenda, acknowledging the potential impact of these new technologies. As a result of the Working Group's deliberations, the Administration released the *Framework for Global Electronic Commerce* in July 1997. The Framework established a series of principles to guide the digital economy of the future. In general, these principles supported private sector leadership and minimal Government intervention on EC; when Government involvement is needed, it should be directed at providing a predictable legal environment. In addition, it called for a decentralized, technology-neutral approach to policy and called for international agreements to create a global EC marketplace.[11] The *Presidential Directive on Electronic Commerce* was issued on July 1, 1997, providing a strategy for the various departments and agencies implementing the Framework. The Working Group is overseeing the implementation of the Framework. In November 1998, it issued its first annual report. Although the Framework was directed toward general commercial uses of EC, it has also prompted initiatives within the Federal Government to incorporate EC as a core element of business operations.

2.2.2 Initiatives to Incorporate EC Within the Federal Government

Because of shrinking budgets, a decreased workforce, and taxpayer demand for improved performance, the Federal Government has been reengineering its business operations with a focus on streamlining the procurement process. The Federal Government processes 22 million transactions with the private sector each year, accounting for more than $220 billion.[12] An additional 10 million transactions among Federal entities adds another $450 billion to the procurement market. These transactions are typically labor intensive and involve recording a significant amount of information on paper. The Federal Government has realized the potential benefit that EC-related technology could bring its reengineering process. As a result, a series of

[11] The U.S. Working Group on Electronic Commerce. *Framework for Global Electronic Commerce*, July 1997.
[12] The President's Management Council Electronic Processes Initiatives Committee, *Electronic Commerce for Buyers and Sellers, A Strategic Plan for Electronic Federal Purchasing and Payment*, March 1998, p. 8.

initiatives are underway to incorporate EC into business operations. These initiatives are being driven by the National Performance Review, the President's Management Council, DOD, the FECPO, and the *Government Paperwork Elimination Act of 1998*.

2.2.2.1 The National Performance Review

In February 1997, the National Performance Review released its report, *Access America*, which outlined ways information technology could help the Government deliver services to the public and improve inter-governmental coordination. The report outlined steps to increase citizen and business access to the most commonly requested Government services by using the Internet and other electronic technologies. The report acknowledged that securing these electronic initiatives is critical when it stated, "Public confidence in the security of the Government's electronic information and information technology is essential to creating government services that are more accessible, efficient, and easy to use. Electronic commerce, e-mail, and electronic benefits funds transfer sensitive information within government, between the government and private industry or individuals, and among governments."[13] As a result of the *Access America* report, the Government Information Technology Services (GITS) Board was empowered to determine how to foster a safe and secure environment for electronic initiatives. In September 1998, the GITS Board released *Access with Trust*, a report that focuses on how the Federal Government could promote and safeguard electronic interactions with citizens, industry, and among departments and agencies.

2.2.2.2 The President's Management Council

In March 1998, the President's Management Council's Electronic Processes Initiatives Committee (EPIC) submitted a strategic plan to Congress on using EC within the Federal Government. The President's Management Council, composed of Chief Operating Officers within the Federal Government, submitted the plan in response to a requirement in Section 850 of the fiscal year (FY) 1998 Department of Defense Authorization Act. The plan states that, "by the year 2001, all Federal departments and agencies will support their programs by making available customer-friendly electronic purchasing tools integrated with end-to-end commercial electronic processing of payment, accounting and performance reporting information."[14] To reach this goal, Federal departments and agencies will spend the next 3 years building a consistent structure for EC processes within the industry/Government by:

- improving communications with key partners in the public and private sector,
- ensuring Federal departments and agencies implement commercial EC software and technologies, and

[13] National Performance Review. *Access America*, February 1997.
[14] *The President's Management Council Electronic Processes Initiatives Committee*. Op. cit., p. 8.

- reengineering key functions of the procurement process to strengthen market research capabilities and facilitate more effective negotiations.[15]

2.2.2.3 Department of Defense

Within the NS/EP community, the DOD has taken a lead in proposing the use of EC to streamline its business operations. In November 1997, DOD released the *Defense Reform Initiative Report* (DRI), which outlines measures that the Department will take to change its business practices by incorporating lessons learned from corporate America. A key tenet of the DRI report is to adopt EC technologies to dramatically reduce the amount of paper DOD processes and stores. DOD intends to conduct most of its commercial contracting and purchasing processes using several EC tools such as EDI, electronic funds transfer (EFT), e-mail, Internet technologies, computer bulletin boards, and other electronic means. DOD anticipates that EC applications will facilitate significant changes in DOD's procurement and logistics processes. These electronic processes will move DOD toward a modern business environment in which it can acquire and pay for goods and services more efficiently. The DRI acknowledges a need to move from a "just-in-case" to a "just-in-time" approach to logistics.[16] EC technology can help achieve this objective by merging warehousing and transportation functions to create just-in-time delivery results, eliminating the need to store raw materials and finished components just-in-case. DOD believes this approach will create a more mobile fighting force. The DRI report outlines the following key goals for creating a paperless environment within DOD:

- By January 1, 2000, all aspects of the contracting process for major weapons systems will be paper-free.

- By FY 2000, 90 percent of DOD purchases under $2,500 will be made using the Government-wide International Merchant Purchase Authorization Card (IMPAC). The IMPAC card is a commercial VISA card issued to individual Government offices and organizations for official purposes.

- DOD will expand the use of electronic catalogs.

- Paper-free systems will be created for weapons support and logistics.

- DOD plans to discontinue volume printing of all DOD-wide regulations and instructions and make them available exclusively on the Internet or CD-ROM.[17]

[15] Ibid., p. 8-11.
[16] Department of Defense. *Defense Reform Initiative Report*, November 1997, p. 1.
[17] Ibid., p. 1.

To centralize management of EC initiatives within DOD, JECPO was created and staffed with personnel from the Defense Information Systems Agency (DISA) and the Defense Logistics Agency (DLA). The JECPO is faced with several difficult challenges. DOD has 150 accounting systems, 76 procurement writing systems, several different logistics systems, and a major contract administration and payment system.[18] Few of these systems are integrated. To reach the goal of a paperless procurement environment, JECPO must manage a critical examination of business practices and support processes across these various systems, including how these systems can be linked electronically in a secure environment using state-of-the-art security tools. Similarly, the JECPO must also reach out to DOD's contracting and trading partners, and ensure that they can use state-of-the-art security tools to link to necessary systems.

2.2.2.4 Federal Electronic Commerce Program Office

FECPO was created in 1998 to coordinate, monitor, and report on the various EC initiatives within the Federal Government. It acknowledges that EC is becoming a preferred way of conducting business with the Federal Government. As a result, the office is developing a policy framework to support EC and helping agencies develop their own EC initiatives. The office is co-chaired by representatives from DOD and the General Services Administration (GSA). The co-chairs oversee three teams: (1) the EC Coordination Team, which works with Federal departments and agencies to coordinate and monitor implementation within the Federal Government; (2) the EC Policy Team, which works with Federal departments and agencies, the Office of Management and Budget, EPIC, and other entities on creating policies to support Federal EC initiatives; and (3) the Card Technology Team, which works with agencies on efforts to implement government-wide implementation of card technologies. As EC continues to develop within the Federal Government, the FECPO is likely to play a key role in how various EC initiatives are implemented.

2.2.2.5 Government Paperwork Elimination Act of 1998

On October 21, 1998, Congress passed the *Government Paperwork Elimination Act of 1998*, a measure designed to "enhance electronic commerce by promoting the reliability and integrity of commercial transactions through establishing authentication standards for electronic communications and for other purposes."[19] The President subsequently signed the bill into law. The intent of the law is to "provide a framework for reliable and secure electronic transactions with the Federal Government."[20] In passing the law, Congress stated that the widespread use of

[18] GAO. Testimony Before the Subcommittee on Military Readiness, Committee on National Security, House of Representatives. "Defense Management: Challenges facing DOD in Implementing the Defense Reform Initiatives." March 13, 1998, p. 13.
[19] *Government Paperwork Elimination Act of 1998* (P.L. 105-277).
[20] Senate Committee on Commerce, Science, and Transportation, *Government Paperwork Elimination Act: Report on S. 2107*, Washington, DC, September 17, 1998.

electronic forms would improve the speed and efficiency of Government services. The law states the following:

- Federal agencies must make electronic versions of their reports available on-line and allow individuals and businesses to use digital signatures to file forms electronically according to guidelines established by the Director of OMB and the Secretary of Commerce.

- Forms submitted electronically, using digital signatures, would have the same legal force as written documents.

- The Secretary of Commerce and General Accounting Office (GAO) are required to periodically report on the status of the law.

Because the Act was only recently signed into law, its effect on Federal EC initiatives is unclear; however, it appears to direct the Federal Government toward a possible full-scale use of EC in business operations. The use of EC by Government, industry, and individual consumers is likely to increase during the next decade, particularly in light of the rising number of public and private sector initiatives aimed at encouraging EC. The security risks of EC should be considered as industry, the Federal Government, and the NS/EP community begin to incorporate EC applications on a broader scale.

3.0 ELECTRONIC COMMERCE SECURITY

Continuing advances in technology offer compelling reasons for more organizations to move toward EC. It is likely that EC will become a significant component of essential business operations within the next decade. As this trend persists, it is important that organizations planning to use EC become familiar with information security objectives, the nature of the EC architecture, and vulnerabilities related to EC technologies.

3.1 Security Objectives

In most cases, public and private organizations are planning to implement EC using Internet technologies, which offer faster, more cost-effective, and efficient transactions than the more proprietary systems. Although EC presents clear benefits, legitimate security concerns regarding the Internet and EC applications present significant challenges that must be addressed. Before users will migrate critical operations to EC technology, they must have the confidence that the technology will provide the following:

- *Data confidentiality*: Assurance that data is disclosed only to authorized subjects.[21]
- *Data integrity*: The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. [22]
- *Availability*: The property that a given resource will be usable during a given time period.[23]
- *Reliability*: The probability of a given system performing its mission adequately under the expected operating conditions.[24]
- *Authentication*: Providing assurance regarding the identity of a subject or object; for example, ensuring that a particular user is who he claims to be.[25]

[21] *Computers at Risk: Safe Computing in the Information Age*, System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press, Washington, DC, 1991.
[22] *Glossary for Computer Systems Security, Federal Information Processing Standards Publication (FIPS PUB 39)*, U.S. Department of Commerce, National Bureau of Standards, 1976.
[23] *Computers at Risk: Safe Computing in the Information Age*. Op. Cit.
[24] Glossary of Computer Security Terms, DOD Directive 5200.28-STD, *DOD Trusted Computer System Evaluation Criteria*, National Computer Security Center, October 1988.
[25] *Computers at Risk: Safe Computing in the Information Age*. Op Cit.

- *Nonrepudiation*: An authentication that with high assurance can be asserted to be genuine and that cannot subsequently be refuted.[26]

Without these assurances, business transactions could be disrupted through malicious actions that intentionally block access to a computer system, criminals could break into computer systems and access sensitive information, or information on a computer system or in transit could be altered. Vulnerabilities in information systems may allow intruders to destroy, steal, and modify data; spread malicious code; or shut down networks. These vulnerabilities are exacerbated by the introduction of EC, which exposes new vulnerabilities and potentially places more valued information at risk. The net result is that EC will expose what were once closed and paper-based business processes to the vulnerabilities of the supporting IT technologies; exploitation of such vulnerabilities may have implications for NS/EP operations that rely on EC.

3.2 The EC Architecture

EC incorporates a wide range of business areas such as procurement, logistics, medical, finance, transportation, travel, and paperless contracting. This section examines one area, procurement, in order to present an example of what tools make up an EC architecture. The EC architecture is composed of processing components, communications links, and administrative services that collectively provide an EC solution and must all be accounted for when securing EC. A vulnerability in any of these segments of the EC architecture leaves a critical opening in the system that could be used to disrupt service, compromise data confidentiality, and commit fraud. The communications component of the EC architecture is made up of the lines, routers, Web servers, e-mail Points of Presence (POP), and firewalls involved with transferring business data between various EC processing components. Traditionally, Value Added Networks (VAN) carried out the exchange of electronic data in a variety of formats. However, as documented previously, the commercial expansion of the Internet has led to enormous interest in business-to-business Internet commerce. The communications path for an EC data transaction now typically involves use of the Internet and Hypertext Transfer Protocol (HTTP). Numerous other protocols are also used to transfer information in an EC transaction, such as Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Multipurpose Internet Mail Extensions (MIME). The Internet was not designed for commercial purposes; therefore, it is currently a relatively insecure medium for conducting mission-critical business functions. This situation raises concerns about using the Internet to transfer critical business information.

A number of steps have been taken to help ensure the security of the communications path for EC data transactions. Protocols, such as transmission control protocol (TCP), were designed to interact with the Internet Protocol (IP) to establish a communications path between two computers. Other protocols have been designed to interact with TCP/IP to further ensure the confidentiality and authenticity of data transactions. Protocols such as Secure Socket Layer

[26] *Computers at Risk: Safe Computing in the Information Age*, Op. Cit.

(SSL), Secure Electronic Transactions (SET), Secure Hypertext Transfer Protocol (S-HTTP), and Secure Multipurpose Internet Mail Extensions (S/MIME) have been designed to use strong 56-bit to 128-bit encryption and provide a high level of security for Internet transactions. With these protocols in place, the EC data transaction is relatively secure, leaving criminals to seek the path of least resistance. Vulnerabilities in the other components of the EC architecture—the EC processing components, EC data stores, and human roles—could potentially present such a path of least resistance.

The processing component of the EC architecture is divided into two categories of components, servers and clients, which process and route business information associated with EC transactions. An EC server consists of a Web server, databases, transaction-processing systems, and interface software.[27] The server provides the tools that allow an organization to conduct business with its partners and customers and keep track of transactions. The EC client allows two parties in an EC transaction to communicate and is typically composed of a Web browser or a proprietary software program. Table 1 lists examples of EC processing components.

Table 1. EC Processing Components

Component	Description
Customer Access Equipment	The client that allows two parties to interface with EC servers.
Purchasing Servers	Launch point for electronic buying. Web-based link between individual users (requisitioners) and sellers' Web sites.
Merchant Servers	Electronic storefront, presents the goods for sale and is a means for requisitioner to select items and place an order.
Payment Servers	Process authorizations and capture transactions.
EDI Servers	Used to exchange, translate, and archive standard business transactions (such as X.12) between enterprises.

A key factor to consider when discussing potential vulnerabilities in EC processing components is the type of data accessed and stored in an EC transaction. This data could provide valuable information malicious actors could use for their own gains. Examples of data stored in an EC transaction include the following:

[27] Ghoush, Anup. "Securing the Web Server: Windows NT versus Unix." This paper was submitted to the National Computer Security Association conference, *Electronic Commerce Security*, held in Washington, DC, on August 4, 1997.

- *User Profiles*: Maintained by purchasing organizations. Includes information about the users such as user name, user account, purchasing authorizations, shipping address, electronic mail address, and pre-approved transaction limits. May also be extended to track information on user preferences and buying habits.

- *Trading Partner Databases:* Captures the contractual arrangements between trading partners. Maintained by purchasing and selling organizations, the data contained is the result of trading partner negotiation and registration.

- *Seller's Catalogs:* Also known as electronic storefronts, the catalogs maintain and display contractually defined sets of products and services available to authorized users.

- *Orders:* The information, workflow steps, approvals, account, and tax status information necessary to complete an order.

- *EDI Transactions:* Ongoing and archived business transactions between trading partners.

- *Additional Data Stores:* EC functions must typically interface with legacy accounting, personnel, and inventory systems.

It is critical to note that organizations adopting EC must realize that potential vulnerabilities in EC processing components (e.g., flawed Web servers and browsers, misconfigured operating systems, and inadequate access controls to databases) threaten the robustness of the EC architecture and could provide unauthorized access to sensitive stored information.

The human factor is another critical element affecting the security of the server and client. A typical EC transaction involves a series of administrative services. The following roles must be filled in order to process and route an EC transaction:

- *Requisitioner:* The requisitioner affiliated with the purchasing organization places the orders for the products and/or services.

- *Purchasing Organization:* The purchasing organization manages the processes and information systems that support purchasing, and the communications links to suppliers. The purchasing organization maintains an EDI server for transaction management (e.g., receiving and returning orders, translation, routing, and archiving).

- *Selling Organization:* Each selling organization publishes electronic catalogs listing its goods and/or services and processes orders. Additionally, the selling organization maintains links with the appropriate payment authorities.

- *Payment Authority:* The payment authority provides authorization for the payment vehicle presented by the requisitioner, makes payments to the selling organization and invoices, or debits the buying organization.

Because an EC transaction involves a number of different human interactions, the potential for human error is a critical factor. Often employees have not been trained in software security, and either through error or disregard for organizational data security practices, they can make the architecture more vulnerable to attack.

3.3 Threats to the EC Architecture

The threat to an EC architecture mirrors the traditional threat to information systems. Motives for attacking an EC architecture are as varied as the types of intruders conducting the attacks. Architectures may be attacked for national interests, financial gain, industrial espionage, power, revenge, prestige, ideology, and simple curiosity.[28] Examples of perceived threats to the NS/EP community's potential use of EC include:

- *Errors:* Errors occur when a system user, either through a lack of training or failure to follow established security procedures, performs an action that exacerbates or exploits a vulnerability in the system.[29] This action could lead directly to loss of information on a critical system or expose a system to a vulnerability.

- *Malicious Insiders:* The insider is a significant threat to information system security. Unauthorized access by insiders accounts for nearly 80 percent of information system breaches.[30] The multi-faceted threat includes disgruntled employees, paid informants, compromised or coerced employees, former employees, and contractors. The 1998 NSIE White Paper, "The Insider Threat to Information Systems," noted that insiders have the opportunity, capability, and motivation to attack an information system.[31]

---

[28] NSIE, "An Assessment of the Risk to the Security of the Public Networks." Prepared by the U.S. Government and NSTAC Network Security Information Exchanges, December 12, 1995, p. 11.
[29] Office of the Under Secretary of Defense for Acquisition and Technology, "Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)," November 1996, p. 30, http://www.jya.com/iwdmain.htm
[30] Nichols, Randall K., "Commercial Information Security, Tiger Teams and Encryption." This paper was submitted to the National Computer Security Association conference, *Electronic Commerce Security*, held in Washington, DC, August 4, 1997.
[31] OMNCS, "The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment," prepared by the U.S. Government and NSTAC National Security Information Exchanges, April 1998, p. 4.

- *Foreign Governments:* To support national interests, many countries have established relationships with businesses and Government entities to develop a capability to collect economic, scientific, technological, and military intelligence. The NSIE assessment of the risk to the security of the Public Network pointed out that it is difficult to assess the full magnitude of the threat posed by foreign Government sponsored activities because many companies do not fully document or share their intrusion experiences.[32]

- *Industrial Spies:* Industrial espionage focuses on obtaining research and development strategies, manufacturing and marketing plans, and customer lists.[33] As those industries comprising the critical infrastructures become less regulated (e.g., telecommunications and electric utilities), they are becoming increasingly competitive, which could lead to an increase in industrial espionage.

- *Criminals:* A variety of criminal elements are beginning to attack information systems and networks for immediate financial gain and valuable inside information about business operations or even law enforcement activities. As more organizations use information systems for critical information and financial transactions, it is expected that all levels of criminals will continue to target valuable information systems.[34]

- *Hackers:* The hacker threat involves individuals or groups who have the technical knowledge and an understanding of the processes needed to penetrate information systems. The motivation for hackers ranges from curiosity to financial gain.

Although the threat to EC is diverse, it is important to note that the same advances in information technologies that have spurred the growth of EC have also enabled intruders to attack critical systems. Rapid advances in technology have made computer applications needed to launch an electronic intrusion more affordable, user-friendly, and readily available.[35] In addition, the Internet allows hackers to rapidly disseminate information on vulnerabilities and attack methods, leading to repeated attacks after a vulnerability is found.

Considering the vulnerabilities involved with EC and the potential that those vulnerabilities could be exploited, it is critical for organizations to craft comprehensive plans to protect their critical systems. This plan should involve both administrative and technical tools. Examples of administrative tools include developing a detailed security policy and educating employees on that policy, establishing a central management focal point to oversee security, backing up critical data, and making contingency plans should information systems fail. Technical protection measures

[32] NSIE, "An Assessment of the Risk to the Security of the Public Networks," Op. Cit., p. 10.
[33] Nelson, Jack, "U.S. Firms' '97 Losses to Spies Put at $300 Billion," *Los Angeles Times,* January 12, 1998.
[34] Office of the Under Secretary of Defense for Acquisition and Technology. Op. Cit., p. 30.
[35] OMNCS. "Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document," March 1999.

should begin with access controls such as password protection, properly configured firewalls, or other access devices such as smart cards that protect systems from unauthorized access. In addition, encryption plays a major role in providing technical protection measures. Organizations should consider tools such as SSL or SET, each of which uses encryption to ensure data integrity and data confidentiality. For further protection, organizations should use digital signatures, which use encryption techniques to ensure data integrity and nonrepudiation by allowing recipients of a message to ensure that a sender is authentic. Combining message encryption in the form of SSL with digital signatures can strengthen the security of an EC environment.

4.0 FACTORS AFFECTING ELECTRONIC COMMERCE RISK

As the Federal Government and the NS/EP community migrate to commercial standards and practices through the use of EC, it is important to understand the implications of these emerging commercial trends and how they affect EC risk. This section explores technological and commercial trends that may increase the vulnerability of EC systems. Over the past decade, a number of organizations within the commercial sector have integrated EC into their commercial standards and practices, reflecting a number of characteristics of the introduction of new information technologies. These characteristics include a change in the speed of business, an increase in the rate of technology, the use of commercial-off-the-shelf products (COTS), existing concerns over information security within the Federal Government, and finally issues related to the differing views on risk between the public and private sectors.

4.1 Speed of Business

The commercial world is a highly competitive arena where bringing the best product or service to market quickly is essential. EC benefits organizations by increasing the efficiency of their business operations. Commercial businesses have used advances in EC technology to move from a "just-in-case" to a "just-in-time" approach to logistics. Just-in-case logistics involves storing large quantities of warehoused inventory, just in case they are needed. With advances in EC technologies, organizations can communicate with their suppliers at a much faster rate and suppliers can fulfill their requests "just-in-time." As a result, a new paradigm has emerged. Just-in-time is an inventory management process designed to reduce the warehousing of large quantities of components that may occupy a space for a brief period of time before they are needed. The just-in-time approach takes advantage of the speed and efficiency of EC and merges the warehousing and transportation functions to place components at the manufacturing site or the retail store coincident with the anticipated need for the items, eliminating the need to stockpile components. Organizations can manage their inventories more effectively, reduce operating costs, improve customer service, and react quickly to changes in customer demand. Recognizing how just-in-time logistics has revolutionized the commercial sector, the DOD has taken steps to incorporate EC and establish a new logistics mindset within the U.S. military.[36]

4.2 Rate of Technology Change

We are living in a world of incredible technology change. In 1983, when the personal computer was becoming more widely adopted, the life-cycle of technology was about 5 years. Today, rapid advances in information technology have dramatically reduced the life cycle to 6 to 8 months. This has caused problems in planning for the introduction of new technologies and practices. Historically, the strategic planning time frame has been 3 to 5 years; the operational planning time frame has been 1 to 3 years. Rapid advances in technology have compressed these planning

[36] Department of Defense. *Defense Reform Initiative Report*, November 1997.

cycles, reducing the strategic planning time frame to 1 year and operational planning time frame to a matter of a few months. Organizations now run the risk of using technologies before they have developed the methodologies and practices needed to support those technologies. Electronic commerce encompasses a wide variety of new and emerging technologies. Incorporating EC involves introducing a whole new set of technologies that reengineer business operations. To implement EC successfully, organizations must be sufficiently flexible to develop effective methodologies and practices to support new EC technologies within the short time frame demanded by the rapid rate of technological change and a compressed planning cycle.

4.3 Commercial-Off-the-Shelf Products

Organizations incorporating EC are doing so largely by using COTS software and hardware products. These organizations are turning to COTS products primarily because they are less expensive than custom-built components. Examples of COTS products include Web servers, browsers, operating systems, and database systems. Several general security issues exist in the use of COTS products. From an end-user, consumer point-of-view, COTS products tend to be generic solutions for non-specific problems. Consumers have little or no ability to affect the design, development, or testing of any COTS products. Although such products promote consistent business practices, which is a distinct advantage, they do not accommodate unique business processes. Continuing upgrades are available for major software products, but these are designed to address the needs of the widest population and are not tailored to the unique needs of a single business. Organizations using COTS products must be ready and able to reengineer their business operations to accommodate the software.

In addition, the COTS market is largely influenced by availability. Generally, the first product to market has the greatest opportunity to gain market share and establish a standard for that product. Because fixes are often bundled with new releases and upgrades, the problem of applying the needed solution is further complicated by the uncertainties of the robustness and pre-testing of the new release and its effect on system performance.[37] As a result, the industry is pressed to release a product in a relatively short time and sometimes is forced to reduce the time spent in testing the product.[38] This leads to flaws in product design that could introduce vulnerabilities to a system. As COTS components with design flaws are replicated throughout the market, the vulnerabilities are also replicated throughout a wide section of end users. Although design flaws are generally discovered and fixes distributed, organizations may not be aware of them and are generally unable, and sometimes unwilling, to implement needed fixes. This problem degrades system integrity, leaving it vulnerable to technological failure or to attack because malicious actors are often aware of product design flaws and exploit them. Therefore, organizations using COTS products to incorporate EC need to be alert to potential design flaws and stand ready to

[37] Computer Science and Telecommunications Board, National Research Council. *Trust in Cyberspace.* Washington, DC: National Research Council Press, January, 1999, Chapter 3, pp.102-103
[38] Ibid., p.101.

implement necessary fixes. In particular, the NS/EP community must stand alert as it shifts from using products built according to its own standards toward using COTS products over which it has little, if any, control.

4.4 Federal Government Information Security

In addition to the vulnerabilities affecting the use of EC in the commercial sector, several trends are operating within the Federal Government that could significantly affect Federal departments and agencies as they adopt EC. The Federal Government's reliance on information systems has been growing over the past decade. Many of the essential functions performed by the Government, such as procurement, logistics, and benefit disbursement, already depend on electronic data and automated information systems. More services that support national defense and law enforcement are also using sophisticated information systems because of their cost-effectiveness, speed, and efficiency. However, there are questions concerning the security of those information systems. In a report issued September 1998, the GAO summarized audit reports issued by the agency from March 1996 through August 1998 that had found substantial weaknesses in the security of information networks in 24 agencies. The September 1998 GAO report said, "Significant information security weakness were identified in each of the 24 agencies covered by our analysis—agencies that in fiscal year 1997 accounted for 99 percent of reported Federal outlays."[39] Poor control over the access to sensitive data and systems was the mostly widely reported weakness discovered by GAO audits. Weaknesses in access controls can be exploited to disrupt critical operations at these agencies and could place sensitive data and assets at risk.

In addition to the access control issue, the GAO report also found that poor security planning and management was a problem in 17 agencies. Of the agencies noted in the report, most have begun to develop policies and procedures to address their information security weaknesses but questions exist about the effectiveness of these policies and whether these policies are based on an adequate assessment of risk. Many Federal departments and agencies still need to establish a framework within their organization for identifying and assessing risks to their information systems. These information security concerns with Federal departments and agencies raise significant questions as the Government moves to the widespread adoption of EC. The widespread adoption of EC would use many of the same information systems determined by the GAO as having significant security weaknesses. This move could potentially place even more sensitive information and assets at risk.

[39] GAO, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk,* Washington, DC, September 1998, p. 23.

4.5 Coordination of EC Initiatives

Various Federal departments and agencies over the past few years have recognized the benefits that EC would bring to their business operations. Government managers have begun to implement EC within their own organizations on an ad hoc basis, often using policies and procedures that differ from those of other departments and agencies. This practice has created interoperability problems within the Federal Government and between the Federal Government and its partners in the private sector. This situation has led to an effort to standardize the move to EC by creating within the Federal Government a "single face to industry." Initiatives by the President's Management Council, DOD, GSA, and FECPO have sought to create policies and procedures to standardize Federal EC programs. However, differences in agency missions and needs have shown that standardization is difficult and coordination of EC efforts at this time is elusive. Standardizing EC operations among departments and agencies with disparate missions is difficult in the absence of a strong entity within the Government to coordinate EC efforts. Coordination is key in developing a standard baseline of EC security throughout the Government. Accordingly, the overall security associated with EC may be compromised by stakeholders with disparate security concerns and approaches.

4.6 Risk Approaches

The commercial sector makes business decisions based on how the decision will affect the bottom line (profitability, shareholders, market share, etc.). Decisions are based upon a business case, with an understanding that some degree of risk must be accepted. Many businesses have decided that the overall benefit of EC outweighs the potential risks. The commercial sector generally has a higher tolerance for risk than the Government has traditionally had. Although the commercial sector acknowledges threats and vulnerabilities, cost-effectiveness is the driving factor in deciding how to mitigate vulnerabilities. Even with the vulnerabilities that are introduced, given the nature and speed of business change and the accelerating rate of technology change, it is clear that EC is becoming a critical component of commercial business operations. Many of the vulnerabilities and trends affecting EC and discussed in this analysis are likely to persist for the next decade, if not longer.

Historically, the Federal Government has tended to have a lower tolerance of risk, almost practicing risk avoidance. The objective had been a continuing practice of attempting to eliminate *all* vulnerabilities and develop protection measures against *all* postulated threats. However, with the deployment of new technologies, the Government has acknowledged that it must move away from a risk avoidance mentality.[40] This changing philosophy needs time to permeate throughout the culture of the Federal Government. However, contention among various Government entities as to what constitutes "acceptable risk" may stall this process. The benefits of incorporating EC

[40] The Joint Security Commission. *Redefining Security: A Report to the Secretary of Defense and the Director of the Central Intelligence Agency*, February 28, 1994, Washington, DC.

may be too great for the Federal Government to reject what EC offers. Consequently, the Government should not avoid EC because of its potential risks; rather, it should determine the acceptable level of risk and implement measures that will achieve that objective.

5.0 CONCLUSIONS

The focus of this report is to identify NS/EP issues related to recent activities within the Federal Government to incorporate EC into business operations. The NSTAC focused on how the transition to EC could affect the departments and agencies that conduct NS/EP functions. The analysis assessed how the use of EC would affect: (1) mission-critical operations necessary to respond to an NS/EP event or crisis; and (2) general operational activities that, if disrupted, might impair the ability of Federal departments and agencies to fulfill their NS/EP responsibilities.

Various departments and agencies within the Federal Government have used different forms of EC and EDI for many years. However, recent Federal EC initiatives have marked a change from previous efforts based on scale and technologies used. These efforts mark one of the first forays into incorporating EC on a government-wide scale. As the NS/EP community transitions to EC for business operations, departments and agencies should be alert to a number of issues that could affect how EC is implemented.

5.1 Anticipated Growth of NS/EP Dependence on EC

Initial analysis shows that the NS/EP community's current use of, and dependence on, EC is modest at best. The recent move to incorporate EC using commercial standards is still very early in the process, marked by nearly 30 EC pilot programs within various departments and agencies. At this stage, determining tangible results from either the success or failure of these programs may be premature. However, a number of factors drive the NS/EP community to incorporate EC into its business operations. As noted earlier, many private organizations have been using EC applications for several years and have experienced tangible improvement to their overall business operations. Industry has demonstrated that electronic capabilities, such as Internet-based EC, offer a cost-effective and efficient means to conduct business. The Federal Government has taken note of this trend and is reengineering its processes to exploit the benefits of EC. The NS/EP community has been hesitant to move to EC because of concerns over its security. Private industry's use of EC and its desire to conduct business with the Government electronically will continue to affect EC efforts within the Government. Based on the sheer number of initiatives and champions of EC within the Government, it appears that the use of EC will increase over the next decade. The NS/EP community may find its hesitance to use EC to support its mission overcome by events. Consequently, NS/EP dependence upon EC, while modest at this time, is likely to grow steadily over the next decade.

5.2 Exposure to EC Risks and Vulnerabilities

EC exposes what were once closed and paper-based business processes to the vulnerabilities of EC processing components and supporting information technologies. EC relies on information systems and an underlying communications medium (e.g., the Internet and PN). Vulnerabilities can exist within any of these segments. Incorporating EC into an organization's business operations introduces additional vulnerabilities that have the potential to affect the robustness of information systems and could allow unauthorized access to sensitive stored information. These vulnerabilities could be caused by design flaws in EC processing components, errors in implementing EC components, and human error.

Because the Federal Government's use of EC is relatively new, it is difficult to determine how vulnerabilities in EC technologies might affect Government operations. The move toward EC could potentially place sensitive information and assets at greater risk. The uncertainty related to EC vulnerabilities requires a new approach to risk management. This new approach must address new vulnerabilities, threats, and consequences, and reconsider what constitutes an acceptable level of risk. It is important for the NS/EP community to be aware of the vulnerabilities and make informed decisions regarding how EC technologies should be implemented to achieve an acceptable level of risk.

5.3 Understanding NS/EP Dependence on EC

As the NS/EP community considers and adopts additional processes that require EC, it becomes increasingly important to assess the extent of this dependence and to determine potential consequences. At this stage, many departments and agencies in the NS/EP community may not fully understand their current or future EC dependencies, and consequently could fail to take adequate measures to protect their infrastructures. This new electronic environment is marked by dramatic changes caused by the dependence on technology; a new paradigm of just-in-time logistics; new procurement systems; and a change in relationships among manufacturers, suppliers, vendors, and customers. The NS/EP community will be required to develop a policy framework and reconfigure its systems to adapt to the dynamic electronic environment. This effort will require the NS/EP community to thoroughly assess its current and future dependence on EC applications and architectures, the security requirements and capabilities of its mission-critical networks, and the effect EC will have on its overall business operations. Once EC measures are adopted, the burden is on each department or agency to continually stay aware of the operations affected by EC and develop methodologies and practices to mitigate vulnerabilities.

5.4 Shared Risk

The Federal Government will face a new challenge as it integrates EC into its business operations and the boundaries of its new EC systems extend into the information infrastructures of its commercial business partners. An organization's security solution can be viewed as a chain that is only as strong as its weakest link. As the Government adds trusted users, systems, and/or networks (through outsourcing, business partnering, etc.), security in the emerging electronic environment very much depends on the shared burden of security by any interconnected component.

It is critical to note that in the new electronic environment created by EC, the NS/EP community will depend on commercial products and an information infrastructure that it does not own and operate. Recent EC initiatives move away from using Government developed technologies and standards toward using commercial products and standards, where the Government has little, if any, control over their development. Therefore, the Federal Government and its partners in the private sector must share the NS/EP risks involved with EC. The public and private sector, together, will need to ensure that they build robust and reliable networks and secure their information.

5.5 Lack of Unified Focus on NS/EP-Specific Needs

A number of organizations provide management and administration oversight for implementing EC within the Federal Government, including the JECPO, FECPO, President's Management Council (PMC), Office of Federal Procurement Policy (OFPP), and Federal Electronic Commerce Acquisition Team (ECAT). The lack of a unified and specific focus on NS/EP-related EC needs among these organizations could lead to a lack of formal guidance, policy, procedures, and accountability related to NS/EP needs. Coordination is key in developing a standard baseline of EC security throughout the Government that would allow the NS/EP community to meet its critical functions in the new, emerging electronic environment. It is essential that public and private organizations assisting with administration, implementation, and management of EC be made aware of the NS/EP community's needs. The NS/EP community should increase NS/EP awareness among the various EC management organizations and continue to proceed cautiously on use of, and dependence on, EC.

Concurrent with this effort by the IIG, the NSTAC's Network Group (NG) has been conducting a broad study addressing the overall NS/EP dependence upon the Internet. The report examines not only the extent to which NS/EP operations will directly and indirectly depend on the Internet over the next 3 years, but also how NS/EP operations might be affected by Internet failures. The NG has developed recommendations proposed to help increase the NS/EP community's awareness and understanding of Internet dependencies, technologies, and vulnerabilities, and to encourage NS/EP awareness among Internet organizations and initiatives. In particular, one recommendation states that, *"in accordance with responsibilities and existing mechanisms*

established by Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, the President should direct the establishment of a permanent program to address NS/EP issues related to the Internet." This program would work with the NS/EP community to broaden understanding of evolving direct and indirect Internet dependencies and work with key Internet organizations and standards bodies to increase awareness of NS/EP requirements.

Our analysis of NS/EP issues related specifically to EC has found that a major factor driving the increased use of the Internet by the Federal Government is the broad push to incorporate EC into business operations. The IIG believes that a permanent program established to address NS/EP issues related to the Internet would address NS/EP issues related to EC. The focus of this program should include issues specifically related to the use of EC (e.g., vulnerabilities in EC processing components, securing EC architectures, and the need for contingency planning), and raise awareness within the public and private sectors of issues resulting from the emerging NS/EP dependency on EC.

6.0 RECOMMENDATIONS

This analysis reflects the importance of encouraging a broader awareness of NS/EP issues related to the introduction of EC. This report identifies a number of organizations (e.g., FECPO, JECPO, President's Management Council, Office of Federal Procurement Policy, and Federal Electronic Commerce Acquisition Team) that provide management and administration oversight for implementing EC initiatives within the Federal Government. In addition, a number of entities in the private sector (e.g., service providers, hardware and software vendors) perform critical roles by designing, manufacturing, implementing, operating, and maintaining the infrastructures that support EC. The NSTAC has found a lack of focus on NS/EP needs within these various entities. Therefore, there is a need to establish a focal point within the Federal Government to work with these various public and private organizations to increase their awareness of NS/EP issues related to EC.

Our analysis has also found a need to increase the NS/EP community's awareness of the potential vulnerabilities related to EC. Federal departments and agencies should work with a focal point within the Federal Government to evaluate their current and future dependence on EC for NS/EP mission-critical operations and develop plans and programs to address the vulnerabilities related to incorporating EC into business operations. Departments and agencies need to develop a thorough understanding of their existing information architectures as well as vulnerabilities caused by the introduction of EC. Once identified, plans and programs can be established to protect their systems.

6.1 NSTAC Recommendations to the President

- Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* designate a focal point for examining the NS/EP issues related to widespread adoption of EC within the Government.

As noted in Section 5.5, the NSTAC's Network Group has developed recommendations proposed to help increase the NS/EP community's awareness and understanding of Internet dependencies, technologies, and vulnerabilities, and to encourage NS/EP awareness among Internet organizations and initiatives. In particular, one recommendation states that, *"Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, direct the establishment of a permanent program to address NS/EP issues related to the Internet."* The IIG endorses the recommendation to establish such a program and believes such a program would satisfy this recommendation.

- Recommend that the President direct that Federal departments and agencies, in cooperation with an established Federal focal point, assess the effect of EC technologies on their NS/EP operations.

6.2 NSTAC Direction to the IES

NSTAC directs the Industry Executive Subcommittee (IES) to use existing NSTAC mechanisms to support the Government's efforts in raising awareness of NS/EP issues related to EC.

APPENDIX A

REPORT CONTRIBUTORS

PARTICIPANTS

Unysis	Dr. Dan Wiener, IIG Chair
MCI WorldCom	Mr. Mike McPadden, Task Chair
CSC	Mr. Guy Copeland
GTE	Mr. Lowell Thomas
	Ms. Ernie Gormsen
ITT	Mr. Joe Gancie
	Mr. Dave Kelly
NTA	Mr. Bob Burns
SAIC	Ms. Rosemary Dew
TRW	Mr. Bob Lentz
Unisys	Mr. Fred Tompkins
U S WEST	Mr. Jon Lofstedt

OTHER CONTRIBUTORS

Boeing	Mr. Graeber Jordan
DOC	Mr. Roger Baker
	Mr. Bill Belote
	Mr. Paul London
DOD	Mr. Michael Mestrovich
	Mr. Lin Wells
EOP	Mr. Ira Magaziner
FECPO	Mr. Paul Grant
GSA	Mr. Thomas Burke
	Mr. Tom Sellers
JECPO	Ms. Diana Marshall
RST	Mr. Anup Ghoush
UMD	Mr. Don Riley

APPENDIX B

REFERENCES

Magazine/Newspaper/Press Release Articles

Nelson, Jack, "U.S. Firms' '97 Losses to Spies Put at $300 Billion," *Los Angeles Times,* January 12, 1998.

National Security Telecommunications Advisory Committee (NSTAC) Information Infrastructure Group (IIG) Briefings

Administration Efforts to Facilitate Global Electronic Commerce, Ira Magaziner, Senior Policy Advisor to the President, April 1, 1998.

Department of Defense Policies Concerning Electronic Commerce, Dr. Lin Wells, Office of Undersecretary of Defense for Policy, April 1, 1998.

EC Security: Weak Links, Best Defenses, Anup Ghoush, Reliable Software Technologies, June 17, 1998.

Federal Electronic Commerce Program, Paul Grant, Federal EC Program Office, April 22, 1998.

Global Business Interfaces: Integrating EC Business Applications in Global Defense, Dr. Michael Mestrovich, Office of Undersecretary of Defense for Acquisition and Technology, March 11, 1998.

Joint Electronic Commerce Program Office, Diana Marshall, July 17, 1998.

Overview of DOC Internet and EC Programs, Roger Baker and Paul London, DOC, October 8, 1998.

Overview of GSA Internet and EC Programs, Thomas Burke, GSA, October 8, 1998.

The Payoff of the Boeing Web, Graeber Jordan, Boeing, November 6, 1998.

United Nations EC Project, Don Riley, University of Maryland, College Park, October 8, 1998.

Office of the Manager, National Communications System (OMNCS) – Sponsored Documents

An Assessment of the Risk to the Security of the Public Networks, prepared by the U.S. Government and NSTAC Network Security Information Exchanges, December 12, 1995.

Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document, Office of the Manager, National Communications System, March 1999.

The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment, prepared by the U.S. Government and NSTAC National Security Information Exchanges, April 1998.

Office of Priority Telecommunications (OPT), *Telecommunications Service Priority (TSP) Program Service Manual*. NCSM 3-1-1, March 1998.

Other

Computer Science and Telecommunications Board, National Research Council, *Trust in Cyberspace*, Washington, DC: National Research Council Press, January, 1999.

Department of Commerce, *The Emerging Digital Economy*, March 1998.

Department of Defense, *Defense Reform Initiative Report*, November 1997.

Erwin, Blane, et al., *Sizing Intercompany Commerce*, Forrester Research, July 1997.

General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, Washington, DC, September 1998.

General Accounting Office, Testimony Before the Subcommittee on Military Readiness, Committee on National Security, House of Representatives, "Defense Management: Challenges Facing DOD in Implementing the Defense Reform Initiatives," March 13, 1998.

Ghoush, Anup. "Securing the Web Server: Windows NT versus Unix." Paper submitted to the National Computer Security Association conference, *Electronic Commerce Security*, held in Washington, DC, on August 4, 1997.

Glossary for Computer Systems Security, Federal Information Processing Standards Publication (FIPS PUB 39), U.S. Department of Commerce, National Bureau of Standards, 1976.

Glossary of Computer Security Terms, DOD Directive 5200.28-STD, "DOD Trusted Computer System Evaluation Criteria, National Computer Security Center," October 1988.

Government Paperwork Elimination Act of 1998 (P.L. 105-277).

Joint Electronic Commerce Program Office (JECPO), EC/EDI Handbook, http://www.acq.osd.mil/ec/newhandbook/chapter2/chapter2.htm

The Joint Security Commission. *Redefining Security: A Report to the Secretary of Defense and the Director of the Central Intelligence Agency*, February 28, 1994, Washington, DC.

National Performance Review, *Access America*, February 1997.

Nichols, Randall K., "Commercial Information Security, Tiger Teams and Encryption," paper submitted to the National Computer Security Association conference, *Electronic Commerce Security*, held in Washington, DC, August 4, 1997.

Office of the Under Secretary of Defense for Acquisition and Technology, *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)*, November 1996.

The President's Management Council Electronic Processes Initiatives Committee, *Electronic Commerce for Buyers and Sellers, A Strategic Plan for Electronic Federal Purchasing and Payment*, March 1998.

Senate Committee on Commerce, Science, and Transportation, *Government Paperwork Elimination Act*: Report on S. 2107, September 17, 1998.

System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, Washington, DC, 1991.

The U.S. Working Group on Electronic Commerce, *Framework for Global Electronic Commerce*, July 1997.